GEKP

20 - 235

JS 44 (Rev. 02/19)

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

20 235

I. (a) PLAINTIFFS

Janeka Peace, individually & on behalf of all other similarly situated

(b) County of Residence of First Listed Plaintiff New Castle, DE
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*

Mark S. Goldman | Goldman Scarlato & Penny P.C.| 161 Washington St, Suite 1025, Conshohocken, PA 19428 | (484) 342-0700

DEFENDANTS

Wawa, Inc.

County of Residence of First Listed Defendant Delaware County, PA
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ☐ 1 U.S. Government Plaintiff
- ☐ 3 Federal Question *(U.S. Government Not a Party)*
- ☐ 2 U.S. Government Defendant
- ☒ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*
(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	☐ 1	☐ 1	Incorporated *or* Principal Place of Business In This State	☐ 4	☒ 4
Citizen of Another State	☒ 2	☐ 2	Incorporated *and* Principal Place of Business In Another State	☐ 5	☐ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

Click here for: Nature of Suit Code Descriptions.

CONTRACT	TORTS		FORFEITURE/PENALTY	BANKRUPTCY	OTHER STATUTES
☐ 110 Insurance	PERSONAL INJURY	PERSONAL INJURY	☐ 625 Drug Related Seizure of Property 21 USC 881	☐ 422 Appeal 28 USC 158	☐ 375 False Claims Act
☐ 120 Marine	☐ 310 Airplane	☐ 365 Personal Injury - Product Liability	☐ 690 Other	☐ 423 Withdrawal 28 USC 157	☐ 376 Qui Tam (31 USC 3729(a))
☐ 130 Miller Act	☐ 315 Airplane Product Liability	☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability		PROPERTY RIGHTS	☐ 400 State Reapportionment
☐ 140 Negotiable Instrument	☐ 320 Assault, Libel & Slander	☐ 368 Asbestos Personal Injury Product Liability		☐ 820 Copyrights	☐ 410 Antitrust
☐ 150 Recovery of Overpayment & Enforcement of Judgment	☐ 330 Federal Employers' Liability	PERSONAL PROPERTY	LABOR	☐ 830 Patent	☐ 430 Banks and Banking
☐ 151 Medicare Act	☐ 340 Marine	☒ 370 Other Fraud	☐ 710 Fair Labor Standards Act	☐ 835 Patent - Abbreviated New Drug Application	☐ 450 Commerce
☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans)	☐ 345 Marine Product Liability	☐ 371 Truth in Lending	☐ 720 Labor/Management Relations	☐ 840 Trademark	☐ 460 Deportation
☐ 153 Recovery of Overpayment of Veteran's Benefits	☐ 350 Motor Vehicle	☐ 380 Other Personal Property Damage	☐ 740 Railway Labor Act	SOCIAL SECURITY	☐ 470 Racketeer Influenced and Corrupt Organizations
☐ 160 Stockholders' Suits	☐ 355 Motor Vehicle Product Liability	☐ 385 Property Damage Product Liability	☐ 751 Family and Medical Leave Act	☐ 861 HIA (1395ff)	☐ 480 Consumer Credit
☐ 190 Other Contract	☐ 360 Other Personal Injury		☐ 790 Other Labor Litigation	☐ 862 Black Lung (923)	☐ 485 Telephone Consumer Protection Act
☐ 195 Contract Product Liability	☐ 362 Personal Injury - Medical Malpractice		☐ 791 Employee Retirement Income Security Act	☐ 863 DIWC/DIWW (405(g))	☐ 490 Cable/Sat TV
☐ 196 Franchise				☐ 864 SSID Title XVI	☐ 850 Securities/Commodities/ Exchange
				☐ 865 RSI (405(g))	☐ 890 Other Statutory Actions
REAL PROPERTY	CIVIL RIGHTS	PRISONER PETITIONS	IMMIGRATION	FEDERAL TAX SUITS	☐ 891 Agricultural Acts
☐ 210 Land Condemnation	☐ 440 Other Civil Rights	Habeas Corpus:	☐ 462 Naturalization Application	☐ 870 Taxes (U.S. Plaintiff or Defendant)	☐ 893 Environmental Matters
☐ 220 Foreclosure	☐ 441 Voting	☐ 463 Alien Detainee	☐ 465 Other Immigration Actions	☐ 871 IRS—Third Party 26 USC 7609	☐ 895 Freedom of Information Act
☐ 230 Rent Lease & Ejectment	☐ 442 Employment	☐ 510 Motions to Vacate Sentence			☐ 896 Arbitration
☐ 240 Torts to Land	☐ 443 Housing/ Accommodations	☐ 530 General			☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
☐ 245 Tort Product Liability	☐ 445 Amer. w/Disabilities - Employment	☐ 535 Death Penalty			☐ 950 Constitutionality of State Statutes
☐ 290 All Other Real Property	☐ 446 Amer. w/Disabilities - Other	Other:			
	☐ 448 Education	☐ 540 Mandamus & Other			
		☐ 550 Civil Rights			
		☐ 555 Prison Condition			
		☐ 560 Civil Detainee - Conditions of Confinement			

V. ORIGIN *(Place an "X" in One Box Only)*

☒ 1 Original Proceeding ☐ 2 Removed from State Court ☐ 3 Remanded from Appellate Court ☐ 4 Reinstated or Reopened ☐ 5 Transferred from Another District *(specify)* ☐ 6 Multidistrict Litigation - Transfer ☐ 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing *(Do not cite jurisdictional statutes unless diversity)*:
28 U.S.C §1332(d) - diversity of citizenship under Class Action Fairness Act

Brief description of cause:
Defendants' negligence led to security breach compromising Plaintiff's data

VII. REQUESTED IN COMPLAINT:

☒ CHECK IF THIS IS A CLASS ACTION UNDER RULE 23, F.R.Cv.P.

DEMAND $

CHECK YES only if demanded in complaint:
JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE DOCKET NUMBER

JAN 13 2020

DATE 01/13/2020

SIGNATURE OF ATTORNEY OF RECORD /s/ Mark S. Goldman

FOR OFFICE USE ONLY

RECEIPT # AMOUNT APPLYING IFP JUDGE MAG. JUDGE

GEKP

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA 20 235

DESIGNATION FORM

(to be used by counsel or pro se plaintiff to indicate the category of the case for the purpose of assignment to the appropriate calendar)

Address of Plaintiff: 21 Ridge Drive, New Castle, DE 19720

Address of Defendant: Wawa, Inc. 260 W. Baltimore Pike, Wawa, PA 19063

Place of Accident, Incident or Transaction: Data breach took place at corporate headquarters in Wawa, PA

RELATED CASE, IF ANY:

Case Number: See Attached List of Cases Judge: See Attached List Date Terminated: _____

Civil cases are deemed related when *Yes* is answered to any of the following questions:

1.	Is this case related to property included in an earlier numbered suit pending or within one year previously terminated action in this court?	Yes ☐	No ☐
2.	Does this case involve the same issue of fact or grow out of the same transaction as a prior suit pending or within one year previously terminated action in this court?	Yes ☑	No ☐
3.	Does this case involve the validity or infringement of a patent already in suit or any earlier numbered case pending or within one year previously terminated action of this court?	Yes ☐	No ☐
4.	Is this case a second or successive habeas corpus, social security appeal, or pro se civil rights case filed by the same individual?	Yes ☐	No ☐

I certify that, to my knowledge, the within case ☒ is / ☐ **is not** related to any case now pending or within one year previously terminated action in this court except as noted above.

DATE: 01/13/2020 _____ PA Bar No. 48049

Attorney-at-Law / Pro Se Plaintiff *Attorney I.D. # (if applicable)*

CIVIL: (Place a √ in one category only)

A. Federal Question Cases:	*B. Diversity Jurisdiction Cases:*
☐ 1. Indemnity Contract, Marine Contract, and All Other Contracts	☐ 1. Insurance Contract and Other Contracts
☐ 2. FELA	☐ 2. Airplane Personal Injury
☐ 3. Jones Act-Personal Injury	☐ 3. Assault, Defamation
☐ 4. Antitrust	☐ 4. Marine Personal Injury
☐ 5. Patent	☐ 5. Motor Vehicle Personal Injury
☐ 6. Labor-Management Relations	☐ 6. Other Personal Injury *(Please specify):* _____
☐ 7. Civil Rights	☐ 7. Products Liability
☐ 8. Habeas Corpus	☐ 8. Products Liability – Asbestos
☐ 9. Securities Act(s) Cases	☑ 9. All other Diversity Cases
☐ 10. Social Security Review Cases	*(Please specify):* Negligence- Data Breach
☐ 11. All other Federal Question Cases	
(Please specify): _____	

ARBITRATION CERTIFICATION

(The effect of this certification is to remove the case from eligibility for arbitration.)

I, Mark S. Goldman, counsel of record *or* pro se plaintiff, do hereby certify:

☑ Pursuant to Local Civil Rule 53.2, § 3(c) (2), that to the best of my knowledge and belief, the damages recoverable in this civil action case exceed the sum of $150,000.00 exclusive of interest and costs:

☐ Relief other than monetary damages is sought.

JAN 13 2020

DATE: 01/13/2020 _____ PA Bar No. 48049

Attorney-at-Law / Pro Se Plaintiff *Attorney I.D. # (if applicable)*

NOTE: A trial de novo will be a trial by jury only if there has been compliance with F.R.C.P. 38.

Related Cases

Case No.	Judge	Caption
2:19-cv-06019	Hon. Gene Pratter	Rapak v. Wawa, Inc.
2:19-cv-06032	Hon. Joel Slomsky	Kaufman v. Wawa, Inc.
2:19-cv-06064	Hon. Nitza Quinones Alejandro	Cohen v. Wawa, Inc.
2:19-cv-06076	Hon. Joel Slomsky	Mullen, Angelo & Bauman v. Wawa, Inc.
2:19-cv-06077	Hon. Darnell Jones	Emery v. Wawa, Inc. & Wild Goose Holdings, Co.
2:19-cv-06127	Hon. Gene Pratter	Hans-Arroyo v. Wawa, Inc.
2:19-cv-06142	Hon. Wendy Beetlestone	Muller v. Wawa, Inc.
5:19-cv-06147	Hon. Gene Pratter	Newton v. Wawa, Inc.
19-cv-06161	Hon. Gene Pratter	Roessle v. Wawa, Inc.
19-cv-06179	Hon. Gene Pratter	Fisher v. Wawa, Inc.
19-cv-06190	Hon. Gene Pratter	Schultz v. Wawa, Inc.

GEKP

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

CASE MANAGEMENT TRACK DESIGNATION FORM

JANEKA PEACE	:	CIVIL ACTION
	:	20 235
v.	:	
	:	
WAWA, INC.	:	NO.

In accordance with the Civil Justice Expense and Delay Reduction Plan of this court, counsel for plaintiff shall complete a Case Management Track Designation Form in all civil cases at the time of filing the complaint and serve a copy on all defendants. (See § 1:03 of the plan set forth on the reverse side of this form.) In the event that a defendant does not agree with the plaintiff regarding said designation, that defendant shall, with its first appearance, submit to the clerk of court and serve on the plaintiff and all other parties, a Case Management Track Designation Form specifying the track to which that defendant believes the case should be assigned.

SELECT ONE OF THE FOLLOWING CASE MANAGEMENT TRACKS:

(a) Habeas Corpus – Cases brought under 28 U.S.C. § 2241 through § 2255. ( )

(b) Social Security – Cases requesting review of a decision of the Secretary of Health and Human Services denying plaintiff Social Security Benefits. ( )

(c) Arbitration – Cases required to be designated for arbitration under Local Civil Rule 53.2. ( )

(d) Asbestos – Cases involving claims for personal injury or property damage from exposure to asbestos. ( )

(e) Special Management – Cases that do not fall into tracks (a) through (d) that are commonly referred to as complex and that need special or intense management by the court. (See reverse side of this form for a detailed explanation of special management cases.) (X)

(f) Standard Management – Cases that do not fall into any one of the other tracks. ( )

1/13/2020	Mark S. Goldman	Pltf. Janeka Peace
Date	**Attorney-at-law**	**Attorney for**
(484) 342-0700	484-580-8747	goldman@lawgsp.com
Telephone	**FAX Number**	**E-Mail Address**

(Civ. 660) 10/02

JAN 13 2020

Civil Justice Expense and Delay Reduction Plan
Section 1:03 - Assignment to a Management Track

(a) The clerk of court will assign cases to tracks (a) through (d) based on the initial pleading.

(b) In all cases not appropriate for assignment by the clerk of court to tracks (a) through (d), the plaintiff shall submit to the clerk of court and serve with the complaint on all defendants a case management track designation form specifying that the plaintiff believes the case requires Standard Management or Special Management. In the event that a defendant does not agree with the plaintiff regarding said designation, that defendant shall, with its first appearance, submit to the clerk of court and serve on the plaintiff and all other parties, a case management track designation form specifying the track to which that defendant believes the case should be assigned.

(c) The court may, on its own initiative or upon the request of any party, change the track assignment of any case at any time.

(d) Nothing in this Plan is intended to abrogate or limit a judicial officer's authority in any case pending before that judicial officer, to direct pretrial and trial proceedings that are more stringent than those of the Plan and that are designed to accomplish cost and delay reduction.

(e) Nothing in this Plan is intended to supersede Local Civil Rules 40.1 and 72.1, or the procedure for random assignment of Habeas Corpus and Social Security cases referred to magistrate judges of the court.

SPECIAL MANAGEMENT CASE ASSIGNMENTS
(See §1.02 (e) Management Track Definitions of the
Civil Justice Expense and Delay Reduction Plan)

Special Management cases will usually include that class of cases commonly referred to as "complex litigation" as that term has been used in the Manuals for Complex Litigation. The first manual was prepared in 1969 and the Manual for Complex Litigation Second, MCL 2d was prepared in 1985. This term is intended to include cases that present unusual problems and require extraordinary treatment. See §0.1 of the first manual. Cases may require special or intense management by the court due to one or more of the following factors: (1) large number of parties; (2) large number of claims or defenses; (3) complex factual issues; (4) large volume of evidence; (5) problems locating or preserving evidence; (6) extensive discovery; (7) exceptionally long time needed to prepare for disposition; (8) decision needed within an exceptionally short time; and (9) need to decide preliminary issues before final disposition. It may include two or more related cases. Complex litigation typically includes such cases as antitrust cases; cases involving a large number of parties or an unincorporated association of large membership; cases involving requests for injunctive relief affecting the operation of large business entities; patent cases; copyright and trademark cases; common disaster cases such as those arising from aircraft crashes or marine disasters; actions brought by individual stockholders; stockholder's derivative and stockholder's representative actions; class actions or potential class actions; and other civil (and criminal) cases involving unusual multiplicity or complexity of factual issues. See §0.22 of the first Manual for Complex Litigation and Manual for Complex Litigation Second, Chapter 33.

$400 GEKP

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

JANEKA PEACE, individually and on behalf of all others similarly situated,

Plaintiff,

v.

WAWA, INC.,

Defendant.

20 235

CLASS ACTION COMPLAINT

Case No.

Plaintiff Janeka Peace ("Plaintiff"), individually and on behalf of the Classes defined below, alleges the following against Wawa, Inc. ("Defendant" or "Wawa") based upon personal knowledge with respect to herself and on information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters:

NATURE OF THE CASE

1. Plaintiff brings this class action case against Wawa for its massive failure to secure and safeguard consumers' financial information—allowing malicious software to go undetected on its system for over nine months while millions of customers' sensitive financial data was stolen—and for failing to provide timely notice to Plaintiff and other consumers that their credit card information had been stolen. Plaintiff brings this action on behalf of herself and of the class consisting of all consumers whose credit or debit card information was accessed during the data breach (the "Class Members").

2. On December 19, 2019, Wawa revealed that it had experienced a data security "incident," with its team discovering that "malware" (malicious software) had been on Wawa payment processing servers for more than nine months. According to Wawa, "[t]his malware affected customer payment card information used at potentially all Wawa locations beginning at different

points in time after March 4, 2019 and until it was contained" on December 12, 2019 (the "Data Breach"). Despite servicing between 700 and 800 million customers annually and knowing that gas stations are particularly vulnerable to hacking, Wawa failed to detect the Data Breach for nine months.

3. In fact, one month prior to Wawa's discovery of the malware, Visa—the nation's largest credit card network—warned that fuel dispenser merchants are "an attractive target for criminal threat actors attempting to compromise" credit card data.[1]

4. Wawa believes that the Data Breach exposed customers' payment card information, including credit and debit card numbers, expiration dates, and cardholder names on payment cards used on "potentially all Wawa in-store payment terminals and fuel dispensers" between March and December 2019. As a result, millions of customers were affected at hundreds of retail locations.

5. Wawa violated the rights of Plaintiff and Class members by intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected, failing to disclose to its customers the material fact that it did not have adequate computer systems and security practices to safeguard financial information, failing to take reasonable steps to prevent the Data Breach from occurring, failing to monitor and detect the Data Breach on a timely basis, and failing to provide timely notice after learning of the Data Breach.

6. As a result of the Data Breach, the financial information of the Plaintiff and Class members has been exposed to criminals for misuse. As a direct result of the Data Breach, Plaintiff

[1] *Visa Security Alert, Attacks Targeting Point-Of-Sale At Fuel Dispenser Merchants, November 2019*, available at https://usa.visa.com/dam/VCOM/global/support-legal/documents/visa-security-alert-attacks-targeting-fuel-dispenser-merchant-pos.pdf (last accessed on January 10, 2020).

and Class members suffered, or are likely to suffer, injuries including: the unauthorized use of their financial information; costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts; loss of use of and access to account funds and costs associated with inability to obtain money from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including decreased credit scores and adverse credit notations; costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to ameliorate, mitigate and deal with the actual and future consequences of the Data Breach; and other injuries as more fully set forth below.

7. The injuries to the Plaintiff and Class members were directly and proximately caused by Wawa's failure to implement or maintain adequate data security measures for financial information and failure to timely detect the Data Breach.

8. Further, Plaintiff retains a significant interest in ensuring that her financial information, to the extent it still remains in Wawa's possession, is protected from further breaches, and seeks to remedy the harms she has suffered on behalf of herself and other Class members.

9. Plaintiff brings this action to remedy these harms on behalf of herself and all similarly situated individuals whose financial information was accessed during the Data Breach. Plaintiff seeks the following remedies, among others: reimbursement of out-of-pocket losses, other compensatory damages, any available statutory damages, further and more robust credit monitoring services with accompanying identity theft insurance, and injunctive relief including an order requiring Wawa to implement improved data security measures.

JURISDICTION AND VENUE

10. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million exclusive of

interest and costs. There are more than 100 putative class members. And, at least some members of the proposed Class have a different citizenship from Wawa.

11. This Court has personal jurisdiction over Wawa because it is headquartered in this district, registered and regularly conducts business in Pennsylvania, and has sufficient minimum contacts in Pennsylvania such that Wawa intentionally avails itself of this Court's jurisdiction by conducting operations here and contracting with companies in this District.

12. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to the conduct alleged herein occurred in, were directed to, and/or emanated from this District. Venue is additionally proper because Wawa transacts business and may be found in this District.

PARTIES

13. Plaintiff Janeka Peace is an individual residing in New Castle, Delaware. On January 2, 2020, Plaintiff received an email from her credit card provider informing her that her credit card account was exposed in the Wawa Data Breach, that her credit card was deactivated, and that a new card was being sent to her. As a result, Plaintiff was greatly inconvenienced by spending significant time in resolving this issue, including but not limited to time spent re-establishing automatic payments onto her new credit card account. Moreover, while Plaintiff enrolled in the credit monitoring offered by Wawa, she will require additional credit monitoring and protection beyond the one-year offer.

14. Defendant Wawa, Inc. is a privately owned New Jersey corporation with its principal place of business in Wawa, Pennsylvania. Wawa owns and operates more than 850 convenience retail stores (over 600 of which also operate as gas stations) in Pennsylvania, New Jersey, Delaware,

Maryland, Virginia, Florida, and Washington, D.C. The company has 37,000 employees with approximately $10 billion in revenue, servicing between 700 to 800 million customers annually.

STATEMENT OF FACTS

15. Wawa owns and operates more than 850 convenience retail stores in Pennsylvania, New Jersey, Delaware, Maryland, Virginia, Florida, and Washington, D.C. Wawa is the largest convenience store chain in Greater Philadelphia, and it is also the third-largest retailer of food in Greater Philadelphia.

16. According to Wawa, "at different points in time after March 4, 2019, malware began running on in-store payment processing systems at potentially all Wawa locations." The malware "was present on most store systems by approximately April 22, 2019." But Wawa failed to discover the malware for over nine months after it initially infected Wawa's systems. And, the company did not disclose the Data Breach until December 19, 2019—over a week after it learned of the malware.

17. Wawa believes "this malware no longer poses a risk to customers using payment cards at Wawa." That short-sighted assessment fails to account for (1) the nine month duration of the unlawful access to Class Members' financial information that went completely undetected by Wawa, and (2) the likelihood that Plaintiff and Class Members may still be victimized by fraud and/or identity theft resulting from the Data Breach.

18. Wawa had obligations, arising from promises made to its customers like Plaintiffs and other Class Members, and based on industry standards, to keep sensitive financial information confidential and to protect it from unauthorized disclosures. Class Members provided their financial information to Wawa with the understanding that Wawa would comply with its obligations to keep such information confidential and secure from unauthorized disclosures.

19. Wawa claims it "is fully committed to data security." It further claims to "use security techniques on" its websites, "and through or in connection with our mobile apps or other software- and Internet-enabled programs and services sponsored by Wawa (the 'Sites') to help protect against the loss, misuse or alteration of information collected from [its customers] at the Sites." For a company with revenue in excess of $10 billion, its failure to detect a major financial breach for nine months is clear evidence that its security measures were wholly inadequate.

20. To that end, Visa had previously warned that gas station retail locations (like the hundreds of locations owned and operated by Wawa) were particularly susceptible to financial hacks. Visa recommended a series of steps to be taken to mitigate against potential threats, including but not limited: deploying chip acceptance on point-of-sale devices, deploying point-to-point encryption, implementing network segmentation (to prevent the spread of malware), and importantly, **monitoring networking traffic for suspicious connections and log system/network events.**[2] Wawa's failure to detect malware on its system for nine months is prima facie evidence that it was failing to properly monitor network traffic.

21. Financial information is valuable. A "cyber black market" exists in which criminals openly post stolen payment card numbers and other personal information on many underground Internet websites. Financial information is valuable to identity thieves because they can use victims' personal data for nefarious purposes such as opening new financial accounts and taking out loans in

[2] *Visa Security Alert, Attacks Targeting Point-Of-Sale At Fuel Dispenser Merchants, November 2019*, available at https://usa.visa.com/dam/VCOM/global/support-legal/documents/visa-security-alert-attacks-targeting-fuel-dispenser-merchant-pos.pdf (last accessed on January 10, 2019).

another person's name, incurring charges on existing accounts, or cloning ATM, debit, or credit cards.

22. The Data Breach could easily have been prevented, or at the very least detected soon after the installation of malware. Wawa had the resources to prevent a breach but neglected to adequately invest in data security and to guard against malware.

23. Wawa was well-aware that the financial information it collected, maintained and stored is highly sensitive, susceptible to attack, and could be used for wrongful purposes by third parties.

24. Despite Wawa's knowledge of major data breaches and the heightened risk to gas station payment information, and despite the company being fully aware of the value of financial information on the black market, Wawa's approach to maintaining the privacy and security of the financial information of Plaintiff and Class members was cavalier, reckless, or at the very least, negligent.

25. The ramifications of Wawa's failure to keep Plaintiff's and Class members' financial information secure are severe.

26. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[3] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person."[4] As the FTC recognizes, once identity thieves have personal information, "they

[3] 17 C.F.R § 248.201 (2013).
[4] *Id.*

can drain your bank account, run up your credit cards, open new utility accounts, or get medical treatment on your health insurance."[5]

27. Javelin Strategy and Research reports that identity thieves have stolen $112 billion in the past six years.[6]

28. Reimbursing a consumer for a financial loss due to fraud does not make that individual whole again. On the contrary, identity theft victims must spend time and money repairing the impact to their credit. After conducting a study, the Department of Justice's Bureau of Justice Statistics ("BJS") found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" and resolving the consequences of fraud in 2014.[7]

29. There may be a time lag between when harm occurs versus when it is discovered, and also between when financial information is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[8]

---

[5] Federal Trade Commission, *Warning Signs of Identity Theft*, available at: https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last visited Sept. 12, 2017).

[6] *See* https://www.javelinstrategy.com/coverage-area/2016-identity-fraud-fraud-hits-inflection-point (last accessed on January 10, 2020).

[7] Victims of Identity Theft, 2014 (Sept. 2015) available at: http://www.bjs.gov/content/pub/pdf/vit14.pdf (last accessed on January 10, 2020).

[8] GAO, Report to Congressional Requesters, at 29 (June 2007), available at http://www.gao.gov/new.items/d07737.pdf (last accessed on January 10, 2020).

30. Plaintiff and members of the Class now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their financial information.

31. The Wawa Data Breach was a direct and proximate result of Wawa's failure to properly safeguard and protect Plaintiff' and Class members' financial information from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and the common law, including Wawa's failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff's and Class members' financial information to protect against reasonably foreseeable threats to the security or integrity of such information.

32. As a direct and proximate result of Wawa's wrongful actions and inaction and the resulting Data Breach, Plaintiff and Class members have been placed at an imminent, immediate, and continuing increased risk of harm from financial fraud, requiring them to take the time, which they otherwise would have dedicated to other life demands, such as work, and effort to mitigate the actual and potential impact of the Data Breach on their lives including by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports. This time has been lost forever and cannot be recaptured, and it is certainly compensable.

33. Wawa has only offered a single year of credit monitoring to its customers, despite it being well known and acknowledged that damage and fraud from a data breach can take many years to occur. The additional cost of adequate and appropriate coverage, or insurance, against the losses and exposure that Wawa's actions have created for Plaintiff and Class members, is ascertainable and is a

determination appropriate for the trier of fact. Wawa has also not offered to cover any of the damages sustained by Plaintiff or Class members.

34. While the financial information of Plaintiff and members of the Class has been stolen, Wawa continues to hold financial information of consumers, including Plaintiff and Class members. Particularly because Wawa has demonstrated an inability to prevent a breach, Plaintiff and members of the Class have an undeniable interest in ensuring that their financial information is secure, remains secure, and is not subject to further theft.

35. As a result of the Data Breach, Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of future fraud and misuse posed by her financial information being placed in the hands of criminals who have already, or will imminently, misuse such information. Plaintiff's financial information was potentially exposed for many months while Wawa failed to detect malware on its system.

36. Additionally, Plaintiff suffered actual injury in the form of damages to and diminution in the value of her financial information—a form of intangible property that was compromised in and as a result of the Data Breach.

37. Moreover, Plaintiff has a continuing interest in ensuring that her private information, which remains in the possession of Wawa, is protected and safeguarded from future breaches.

CLASS ALLEGATIONS

38. Plaintiff seeks relief on behalf of herself and as representative of all others who are similarly situated. Pursuant to Fed. R. Civ. P. 23(a), (b)(2), (b)(3) and (c)(4), Plaintiff seeks certification of a nationwide class defined as follows:

> All persons residing in the United States whose financial information was exposed in the data breach announced by Wawa on December 19, 2019 (the "Nationwide Class").

39. Pursuant to Fed. R. Civ. P. 23, and in the alternative to claims asserted on behalf of the Nationwide Class, Plaintiffs assert claims under the laws of the individual States on behalf of citizens of those states, respectively, and on behalf of separate statewide classes, defined as follows:

> All persons residing in [STATE] whose financial information was exposed in the data breach announced by Wawa on December 19, 2019 (the "Statewide Classes"). Excluded from each of the above Classes are Wawa and any of its affiliates, parents or subsidiaries; all employees of Wawa; all persons who make a timely election to be excluded from the Class; government entities; and the judges to whom this case is assigned and their immediate family and court staff.

40. Plaintiff hereby reserves the right to amend or modify the class definition with greater specificity or division after having had an opportunity to conduct discovery.

41. Each of the proposed Classes meets the criteria for certification under Federal Rule of Civil Procedure 23(a), (b)(2), (b)(3) and (c)(4).

42. **Numerosity. Fed. R. Civ. P. 23(a)(1).** Consistent with Rule 23(a)(1), the members of the Class are so numerous and geographically dispersed that the joinder of all members is impractical. While the exact number of Class members is unknown to Plaintiff at this time, the proposed Class includes at least several million individuals whose financial information was compromised in the Data Breach. Class members may be identified through objective means. Class members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods pursuant to Fed R. Civ P. 23(c)(2), which may include U.S. mail, electronic means, or other appropriate means.

43. **Commonality. Fed. R. Civ. P. 23(a)(2) and (b)(3).** Consistent with Fed. R. Civ. P. 23(a)(2) and with 23(b)(3)'s predominance requirement, this action involves common questions of law and fact that predominate over any questions affecting individual Class members. The common questions include:

a. Whether Wawa had a duty to protect financial information;

b. Whether Wawa knew or should have known of the susceptibility of its data security systems to a data breach;

c. Whether Wawa's security measures to protect its systems were reasonable in light of the measures recommended by data security experts;

d. Whether Wawa was negligent in failing to implement reasonable and adequate security procedures and practices;

e. Whether Wawa's failure to implement adequate data security measures allowed the breach to occur;

f. Whether Wawa's conduct constituted deceptive trade practices under various state laws;

g. Whether Wawa's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the loss of the financial information of Plaintiff and Class Members;

h. Whether Plaintiff and Class members were injured and suffered losses because of Wawa's failure to reasonably protect financial information; and

i. Whether Plaintiff and Class Members are entitled to relief, including damages and/or injunctive relief and/or declaratory relief.

44. **Typicality. Fed. R. Civ. P. 23(a)(3).** Consistent with Fed. R. Civ. P. 23(a)(3), Plaintiff's claims are typical of those of other Class members. Plaintiff's financial information was compromised in the Data Breach. Plaintiff's damages and injuries are akin to other Class members and Plaintiff seeks relief consistent with the relief of the Class.

45. **Adequacy. Fed. R. Civ. P. 23(a)(4).** Consistent with Fed. R. Civ. P. 23(a)(4), Plaintiff is an adequate representative of the Class because Plaintiff is a member of the Class and is committed to pursuing this matter against Wawa to obtain relief for the Class. Plaintiff has no conflicts of interest with the Class. Plaintiff's Counsel are competent and experienced in litigating class actions, including privacy litigation. Plaintiff intends to vigorously prosecute this case and will fairly and adequately protect the Class' interests.

46. **Superiority. Fed. R. Civ. P. 23(b)(3).** Consistent with Fed. R. Civ. P 23(b)(3), a class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The quintessential purpose of the class action mechanism is to permit litigation against wrongdoers even when damages to individual Plaintiff may not be sufficient to justify individual litigation. Here, the damages suffered by Plaintiff and the Class are relatively small compared to the burden and expense required to individually litigate their claims against Wawa, and thus, individual litigation to redress Wawa's wrongful conduct would be impracticable. Individual litigation by each Class member would also strain the court system. Individual litigation creates the potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

47. **Injunctive and Declaratory Relief.** Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2) and (c). Defendant, through its uniform conduct, has acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the Class as a whole.

48. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Wawa failed to timely notify the public of the Data Breach;

b. Whether Wawa owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their financial information;

c. Whether Wawa's security measures were reasonable in light of data security recommendations, and other measures recommended by data security experts;

d. Whether Wawa failed to adequately comply with industry standards amounting to negligence;

e. Whether Defendant failed to take commercially reasonable steps to safeguard the financial information of Plaintiff and the Class members; and,

f. Whether reasonable adherence to data security recommendations, and measures recommended by data security experts would have prevented or mitigated the Data Breach.

49. Finally, all members of the proposed Classes are readily ascertainable. Wawa has access to information regarding the Data Breach, the time period of the Data Breach, and which individuals were affected. Using this information, the members of the Class can be identified and their contact information ascertained for purposes of providing notice to the Class.

COUNT I
Negligence

50. Plaintiff restates and realleges Paragraphs 1 through 49 as if fully set forth herein.

51. Upon accepting and storing the financial information of Plaintiff and Class Members in its computer systems and on its networks, Wawa undertook and owed a duty to Plaintiff and Class Members to exercise reasonable care to secure and safeguard that information and to use commercially reasonable methods to do so. Wawa knew that the financial information was private and confidential and should be protected as private and confidential.

52. Wawa owed a duty of care not to subject Plaintiff and Class Members to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

53. Wawa owed numerous duties to Plaintiff and to members of the Nationwide Class, including the following:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting financial information in its possession;

b. to protect financial information using reasonable and adequate security procedures and systems that are compliant with industry-standard practices; and

c. to implement processes to quickly detect a data breach and to timely act on warnings about data breaches.

54. Wawa had a special relationship with Plaintiff and Class members by virtue of its obtaining and storing their financial information. Moreover, only Wawa had the ability to protect its systems and the financial information it stored on them from attack.

55. Wawa's conduct also created a foreseeable risk of harm to Plaintiff and Class members and their financial information. Wawa's misconduct included failing to: (1) secure its systems, despite knowing their vulnerabilities, (2) comply with industry standard security practices, (3)

implement adequate system and event monitoring, and (4) implement the systems, policies, and procedures necessary to prevent this type of data breach.

56. Wawa also had independent duties under state and federal laws that required Wawa to reasonably safeguard Plaintiff's and Class members' financial information and promptly notify them about the Data Breach.

57. The law further imposes an affirmative duty on Wawa to timely disclose the unauthorized access and theft of the financial information to Plaintiff and the Class so that Plaintiff and Class members can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their financial information.

58. Wawa knew, or should have known, of the risks inherent in collecting and storing financial information, the vulnerabilities of its data security systems, and the importance of adequate security. Wawa knew about numerous, well-publicized data breaches.

59. Wawa knew, or should have known, that its data systems and networks did not adequately safeguard Plaintiff's and Class members' financial information.

60. Wawa breached its duties to Plaintiff and Class members in numerous ways, including:

a. by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard financial information of Plaintiff and Class members;

b. by failing to use reasonable care to adequately protect and secure financial information of Plaintiff and Class members during the time it was within Wawa's possession or control;

c. by creating a foreseeable risk of harm through the misconduct previously described;

d. by failing to provide adequate supervision and oversight of the financial information with which they were and are entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted an unknown third party to gather financial information of Plaintiff and Class members, misuse the financial information and intentionally disclose it to others without consent;.

e. by knowingly disregarding standard information security principles, despite obvious risks, both before and during the period of the Data Breach; and

f. by failing to timely and accurately disclose that Plaintiff's and Class Members' financial information had been improperly acquired or accessed.

61. Wawa breached its duty to Plaintiff and Class Members by failing to detect malware on its systems for over nine months and then waiting another week to notify Plaintiff and Class Members about the Data Breach. Unlawful access was therefore ongoing for more than nine months, unbeknownst to Plaintiff and Class Members.

62. Further, through its failure to provide timely and clear notification of the Data Breach to consumers, Wawa prevented Plaintiff and Class members from taking meaningful, proactive steps to secure their financial data and bank accounts and protect against credit fraud or harmful impacts to their credit ratings.

63. Wawa's conduct was negligent and departed from all reasonable standards of care, including, but not limited to: failing to adequately protect the financial information; failing to conduct regular security audits; failing to provide adequate and appropriate supervision of persons having access to financial information of Plaintiff and Class members; and failing to provide Plaintiff and

Class members with timely and sufficient notice that their sensitive financial information had been compromised.

64. Neither Plaintiff nor the other Class members contributed to the Data Breach and subsequent misuse of their financial information as described in this Complaint.

65. As a direct and proximate cause of Wawa's conduct, Plaintiff and the Class suffered damages including, but not limited to: damages arising from the unauthorized charges on their debit or credit cards or on cards that were fraudulently obtained through the use of the financial information of Plaintiff and Class members; damages arising from Plaintiff's and Class members' inability to use their debit or credit cards because those cards were cancelled, suspended, or otherwise rendered unusable as a result of the Data Breach and/or false or fraudulent charges stemming from the Data Breach, including but not limited to late fee charges and foregone cash back rewards; damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, inter alia, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy. The nature of other forms of economic damage and injury may take years to detect, and the potential scope can only be assessed after a thorough investigation of the facts and events surrounding the theft mentioned above.

COUNT II
Negligence Per Se

66. Plaintiff restates and realleges Paragraphs 1 through 65 as if fully set forth herein.

67. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Wawa, of failing to use reasonable measures to protect financial information. The FTC publications and orders described above also form part of the basis of Wawa's duty in this regard.

68. Wawa violated Section 5 of the FTC Act by failing to use reasonable measures to protect financial information and not complying with applicable industry standards, as described in detail herein. Wawa's conduct was particularly unreasonable given the nature and amount of financial information it obtained and stored, and the foreseeable consequences of a data breach at a corporation such as Wawa, including, specifically, the immense damages that would result to Plaintiff and Class members.

69. Wawa's violation of Section 5 of the FTC Act constitutes negligence *per se*.

70. Plaintiff and Class members are within the class of persons that the FTC Act was intended to protect.

71. The harm that occurred as a result of the Wawa Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

72. As a direct and proximate result of Wawa's negligence *per se*, Plaintiff and the Class have suffered, and continue to suffer, injuries arising from Plaintiff's and Class members' inability to use their debit or credit cards because those cards were cancelled, suspended, or otherwise rendered unusable as a result of the Data Breach and/or false or fraudulent charges stemming from the Data Breach, including but not limited to late fee charges and foregone cash back rewards; damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives

including, inter alia, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy.

COUNT III
Violation of the Pennsylvania Unfair Trade Practices and Consumer Protection Law, 73 Pa. Cons. Stat. §§ 201-2 & 201-3, *et seq.*

73. Plaintiff restates and realleges Paragraphs 1 through 72 as if fully set forth herein.

74. Wawa is a "person", as defined by 73 Pa. Cons. Stat. § 201-2(2).

75. Plaintiff and Class Members purchased goods and services in "trade" and "commerce," as defined by 73 Pa. Cons. Stat. § 201-2(3), primarily for personal, family, and/or household purposes.

76. Wawa engaged in unfair methods of competition and unfair or deceptive acts or practices in the conduct of its trade and commerce in violation of 73 Pa. Cons. Stat. Ann. § 201- 3, including:

a. Representing that its goods and services have characteristics, uses, benefits, and qualities that they do not have (73 Pa. Stat. Ann. § 201-2(4)(v));

b. Representing that its goods and services are of a particular standard or quality if they are another (73 Pa. Stat. Ann. § 201-2(4)(vii)); and

c. Advertising its goods and services with intent not to sell them as advertised (73 Pa. Stat. Ann. § 201-2(4)(ix)).

77. Wawa's unfair or deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Class Members' financial information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' financial information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Class Members' financial information, including by implementing and maintaining reasonable security measures and ensuring its vendors and business associates maintained reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' financial information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Class Members' financial

information or ensure its vendors and business associates reasonably or adequately secured such information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' financial information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

78. Wawa's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of its data security and ability to protect the confidentiality of consumers' financial information.

79. Wawa intended to mislead Plaintiff and Class Members and induce them to rely on its misrepresentations and omissions.

80. Had Wawa disclosed to Plaintiff and Class Members that its data systems were not secure and, thus, vulnerable to attack, Wawa would have been forced to use vendors and business associates with reasonable data security measures and comply with the law. Instead, Wawa received, maintained, and compiled Plaintiff's and Class Members' financial information as part of the services it provided without advising Plaintiff and Class Members that its data security practices were insufficient to maintain the safety and confidentiality of Plaintiff's and Class Members' financial information. Accordingly, Plaintiff and Class Members acted reasonably in relying on Wawa's misrepresentations and omissions, the truth of which they could not have discovered.

81. Wawa acted intentionally, knowingly, and maliciously to violate Pennsylvania Unfair Trade Practices and Consumer Protection Law, and recklessly disregarded Plaintiff's and Class Members' rights.

82. As a direct and proximate result of Wawa's unfair methods of competition and unfair or deceptive acts or practices and Plaintiff's and Class Members' reliance on them, Plaintiff and Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; loss of value of their financial information; and an increased, imminent risk of fraud and identity theft.

83. Plaintiff and Class Members seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages of $100 (whichever is greater), treble damages, restitution, attorneys' fees and costs, and any additional relief the Court deems necessary or proper.

COUNT IV
Violation of the Delaware Computer Security Breach Act,
6 Del. Code Ann. §§ 12B- 102, *et seq*.

84. Plaintiff restates and realleges Paragraphs 1 through 83 as if fully set forth herein.

85. Wawa is a business that owns or licenses computerized data that includes Personal Information as defined by 6 Del. Code Ann. § 12B-102(a).

86. Plaintiffs' and Class Members' financial information includes Personal Information as defined by 6 Del. Code Ann. § 12B-101(4).

87. Wawa is required to accurately notify Plaintiffs and Class Members if Wawa becomes aware of a breach of its data security systems which is reasonably likely to result in the misuse of a Delaware resident's personal information, in the most expedient time possible and without unreasonable delay under 6 Del. Code Ann. § 12B-102(a).

88. Because Wawa was aware of a breach of its security system which involved the financial information of Plaintiff and Class Members which is reasonably likely to result in misuse

of Delaware residents' personal information, Wawa had an obligation to disclose the data breach in a timely and accurate fashion as mandated by 6 Del. Code Ann. § 12B-102(a).

89. By failing to disclose the Data Breach in a timely and accurate manner, Wawa violated 6 Del. Code Ann. § 12B-102(a).

90. As a direct and proximate result of Wawa's violations of 6 Del. Code Ann. § 12B-102(a), Plaintiff and Class Members suffered damages, as described above.

91. Plaintiff and Class Members seek relief under 6 Del. Code Ann. § 12B-104, including actual damages and equitable relief.

COUNT V
Violation of the Delaware Consumer Fraud Act,
6 Del. Code §§ 2513, *et seq*.

92. Plaintiff restates and realleges Paragraphs 1 through 91 as if fully set forth herein.

93. Wawa is a "person" that is involved in the "sale" of "merchandise," as defined by 6 Del. Code § 2511(7), (8), and (6).

94. Wawa advertised, offered, or sold goods or services in Delaware and engaged in trade or commerce directly or indirectly affecting the people of Delaware.

95. Wawa used and employed deception, fraud, false pretense, false promise, misrepresentation, and the concealment, suppression, and omission of material facts with intent that others rely upon such concealment, suppression and omission, in connection with the sale and advertisement of merchandise, in violation of 6 Del. Code § 2513(a), including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Class Members' Financial Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks and remediate identified security and privacy risks, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Class Members' Financial Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Delaware's data security statute, 6 Del. Code § 12B-100, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs and Class Members' Financial Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' Financial Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Delaware's data security statute, 6 Del. Code § 12B-100;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Class Members' Financial Information or ensure its vendors and business associates reasonably or adequately secured such information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' Financial Information, including duties

imposed by the FTC Act, 15 U.S.C. § 45, and Delaware's data security statute, 6 Del. Code § 12B-100.

96. Wawa's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of its data security and ability to protect the confidentiality of consumers' Financial Information.

97. Wawa acted intentionally, knowingly, and maliciously to violate Delaware's Consumer Fraud Act, and recklessly disregarded Plaintiffs' and Class Members' rights.

98. Had Wawa disclosed to Plaintiffs and Class Members that its data systems were not secure and, thus, vulnerable to attack, Wawa would have been forced to use vendors and business associates with reasonable data security measures and comply with the law. Instead, Wawa received, maintained, and compiled Plaintiffs' and Class Members' Financial Information as part of the services it provided without advising Plaintiffs and Class Members that its data security practices were insufficient to maintain the safety and confidentiality of Plaintiffs' and Class Members' Financial Information. Accordingly, Plaintiffs and Class Members acted reasonably in relying on Wawa's misrepresentations and omissions, the truth of which they could not have discovered.

99. Wawa's unlawful trade practices were gross, oppressive, and aggravated, and Wawa breached the trust of Plaintiffs and Class Members.

100. As a direct and proximate result of Wawa's unlawful acts and practices, Plaintiffs and Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; loss of value of their financial information; and an increased, imminent risk of fraud and identity theft.

101. Plaintiffs and Class Members seek all monetary and non-monetary relief allowed by law, including damages under 6 Del. Code § 2525 for injury resulting from the direct and natural consequences of Wawa's unlawful conduct; restitution; injunctive relief; and reasonable attorneys' fees and costs.

REQUEST FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all members of the Classes proposed in this Complaint, respectfully request that the Court enter judgment in their favor and against Wawa as follows:

a. For an Order certifying the Classes, as defined herein, and appointing Plaintiff and her Counsel to represent the Nationwide Class, or in the alternative the separate State Classes;

b. For equitable relief enjoining Wawa from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class members' financial information;

c. For equitable relief compelling Wawa to use appropriate cyber security methods, practices, and policies with respect to consumer data collection, storage and protection and to disclose with specificity to class members the type of financial information compromised;

d. For an award of damages, as allowed by law in an amount to be determined;

e. For an award of attorneys' fees, costs and litigation expenses, as allowable by law;

f. For prejudgment interest on all amounts awarded; and

g. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMAND

Plaintiff demands a jury trial on all issues so triable.

Dated: January 13, 2020

GOLDMAN SCARALTO & PENNY, P.C.
Mark S. Goldman
Paul J. Scarlato
161 Washington Street, Suite 1025
Conshohocken, PA 19428
Telephone: (484) 342-0700
Fax: (484) 580-8747
goldman@lawgsp.com
scarlato@lawgsp.com

TADLER LAW LLP
Ariana J. Tadler (*pro hac vice forthcoming*)
Brian R. Morrison (*pro hac vice forthcoming*)
One Penn Plaza, 36th Floor
New York, NY 10119
Telephone: (212) 946-9300
Fax: (929) 207-3746
atadler@tadlerlaw.com
bmorrison@tadlerlaw.com

Counsel for Plaintiff and the Proposed Class